On Universal and Fault-Tolerant Quantum Computing: A Novel Basis and a New Constructive Proof of Universality for Shor's Basis *

P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan †
Electrical Engineering Department
UCLA
Los Angeles, CA 90095

Abstract

*A novel universal and fault-tolerant basis (set of gates) for quantum computation is described. Such a set is necessary to perform quantum computation in a realistic noisy environment. The new basis consists of two single-qubit gates (*Hadamard *and* $\sigma_z^{\frac{1}{4}}$*), and one double-qubit gate (Controlled-NOT). Since the set consisting of Controlled-NOT and Hadamard gates is not universal, the new basis achieves universality by including only one additional elementary (in the sense that it does not include angles that are irrational multiples of* π*) single-qubit gate, and hence, is potentially the simplest universal basis that one can construct. We also provide an alternative proof of universality for the* only other known class *of universal and fault-tolerant basis proposed in [24, 16].*

1. Introduction

A new model of computation based on the laws of quantum mechanics has been shown to be superior to standard (classical) computation models [25, 14]. Potential realizations of such computing devices are currently under extensive research [7, 19, 28, 9, 12, 11, 15, 29], and the theory of using them in a realistic noisy environment is still developing. Two of the main requirements for error-free operations are to have a set of gates that is both universal for quantum computing (see [4] and references therein), and that can operate in a noisy environment (i.e., fault-tolerant) [23, 24, 21, 2, 18, 16].

A scheme to correct errors in quantum bits (qubits) was proposed by Shor [23] by adopting standard coding techniques and modifying them to correct quantum mechanical errors induced by the environment. In such quantum error-correction techniques, the two states of each qubit are encoded using a string of qubits, so that the state of the qubit is kept in a pre-specified two-dimensional subspace of the space spanned by the string of qubits. We refer to this as the logical qubit. This is done in a way that error in one or more (as permitted by the code) physical qubits will not destroy the logical qubit. To avoid errors in the computation itself, Shor [24] suggested performing the computations on the logical qubits (without first decoding them), and this type of computation is known as fault-tolerant computation.

There are a number of requirements that a fault-tolerant quantum circuit must satisfy. To prevent propagation of single-qubit errors to other qubits in the same code word, one requirement of fault-tolerant computation is to disallow operations between any two qubits from the same codeword. This constraint imposes significant restrictions on both the types of unitary operations that can be performed on the encoded logical qubits, and the quantum error-correcting codes that can be used to encode the logical qubits. For example, if a "double-even"

*This work was supported in part by grants from the Revolutionary Computing group at JPL (contract #961360), and from the DARPA Ultra program (subcontract from Purdue University #530–1415–01).

†E–mail addresses of the authors are, respectively: {boykin, talmo, pulver, vwani, vatan}@ee.ucla.edu.

CSS code (e.g., the $((7,2,3))$ quantum code described in [6, 27]) is used then one can show that the following unitary operations can be fault-tolerantly implemented:

$$H,\ {\sigma_z}^{\frac{1}{2}},\ \Lambda_1(\sigma_x) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (1)$$

where H and ${\sigma_z}^{\frac{1}{2}}$ are defined in the next section, and $\Lambda_k(U)$ denotes the controlled–U operation with k control bits (see [4]); $\Lambda_1(\sigma_x)$ is the Controlled-NOT (CNOT) gate. So far, these operations are the only ones that have been shown to be "directly" fault-tolerant (in the sense that no measurements and/or preparations of special states are required) operations. It is well known, however, that the group generated by the above operations (also referred to as the *normalizer group*) is not universal for quantum computation. This leads to the interesting problem of determining a basis that is both universal and can be implemented fault-tolerantly.

There are several well-established results on the universality of quantum bases [1, 3, 4, 5, 8]. Proofs of universality of these bases rest primarily on the fact that they include at least one "non-elementary" gate, i.e., a gate that performs a rotation on single qubits by an irrational multiple of π. A direct fault-tolerant realization of such a gate, however, is not possible; this property makes all the well-known universal bases inappropriate for practical and noisy quantum computation.

The search for universal and fault-tolerant bases has led to a novel basis as proposed in the seminal work of Shor [24]. It includes the Toffoli gate in addition to the above-mentioned generators of the normalizer group; hence, the basis can be represented by the following set $\{\ H,\ {\sigma_z}^{\frac{1}{2}},\ \Lambda_2(\sigma_x)\ \}$. A fault-tolerant realization of the Toffoli gate (involving only the generators of the normalizer group, preparation of a special state, and appropriate measurements) has been shown in [24]; a proof of universality of this basis, however, was not included. Later Kitaev [16] proved the universality of a basis, comprising the set $\{\Lambda_1({\sigma_z}^{\frac{1}{2}}), H\}$ (see Section 5.1), that is "equivalent" to Shor's basis, i.e., the gates in the new basis can be *exactly* realized using gates in Shor's basis and vice-versa.

A number of other researchers have proposed fault-tolerant bases that are equivalent to Shor's basis. Knill, Laflamme, and Zurek [17] considered the basis $\{\ H,\ {\sigma_z}^{\frac{1}{2}},\ \Lambda_1({\sigma_z}^{\frac{1}{2}}),\ \Lambda_1(\sigma_x)\ \}$ and the basis $\{\ {\sigma_z}^{\frac{1}{2}},\ \Lambda_1({\sigma_z}^{\frac{1}{2}}),\ \Lambda_1(\sigma_x)\ \}$ with the ability to prepare the encoded states $\frac{1}{\sqrt{2}}(|0\rangle_L \pm |1\rangle_L)$[1]. The universality of these bases follows from the fact that gates in Shor's basis can be simulated by small size simple circuits over these new bases. Hence, while novel fault-tolerant realizations of the relevant gates in these bases were proposed, no new proofs of universality was required. The same authors later [18] studied a model in which the prepared state $\cos(\pi/8)|0\rangle_L + \sin(\pi/8)|1\rangle_L$ is made available, in addition to the normalizer group gates. Again, the universality of this model follows from the fact that it can realize the gate $\Lambda_1(H)$, and consequently the Toffoli gate. We also note that Aharonov and Ben-Or [2] considered universal quantum systems with basic units that have $p > 2$ states (referred to as qupits). They proposed a class of quantum codes, called polynomial codes, for such systems consisting of qupits. They defined a basis for the polynomial codes and proved that it is universal. However their proof makes explicit use of qupits with more than two states, and hence does not directly apply to the case studied in this paper, where all operations are done on qubits only.

In this paper, we prove the existence of a novel basis for quantum computation that lends itself to an elegant proof (based solely on the geometry of real rotations in three dimensions) of universality and in which all the gates can be easily realized in a fault-tolerant manner. In fact, we show that the inclusion of only one additional single-qubit operation in the set in (1), namely,

$${\sigma_z}^{\frac{1}{4}} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

leads to a universal and fault-tolerant basis for quantum computation. Note that ${\sigma_z}^{\frac{1}{2}}$ is not required anymore. Thus, our basis consists of the following three gates

$$H,\ {\sigma_z}^{\frac{1}{4}}, \Lambda_1(\sigma_x)\ . \quad (2)$$

[1] $|0\rangle_L$ and $|1\rangle_L$ refer to the states of the logical/encoded qubits.

Proving the universality of Shor's basis (see [16]) seems to be a more involved process than proving the universality of the set of gates we suggest here. Moreover, we outline a general method for fault tolerant realizations of a certain class of unitary operations; the fault-tolerant realizations of both the ${\sigma_z}^{\frac{1}{4}}$ and the Toffoli gates are shown to be special cases of this general formulation.

The first part of this paper is devoted to the proof of universality, followed by a discussion on the fault-tolerant realization of the ${\sigma_z}^{\frac{1}{4}}$ gate, and finally an alternate proof for the universality of Shor's basis. We also show in Appendix A that the new basis proposed in this paper is not equivalent to Shor's basis.

2. Definitions and identities

The identity I and the Pauli σ matrices are:

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

We mention the following useful identities: $H := \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$, $\sigma_y = i\sigma_x\sigma_z$, and also, with ${\sigma_z}^{\alpha} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi\alpha} \end{pmatrix}$, we have

$$\sigma_x = H\,\sigma_z\,H \quad \text{and} \quad \sigma_y = {\sigma_z}^{\frac{1}{2}}\,\sigma_x\,{\sigma_z}^{-\frac{1}{2}}\,. \quad (3)$$

We review some properties of matrices in $\mathbf{SU}(2)$. Let $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. Every traceless and Hermitian 2×2 unitary matrix A can be represented as $A = \hat{n} \cdot \vec{\sigma} = n_x\sigma_x + n_y\sigma_y + n_z\sigma_z$, where $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector. From commutation relations $(\hat{n} \cdot \vec{\sigma})^2 = I$, and using this fact, exponentiation of these Pauli matrices can be easily performed, to give

$$e^{i\varphi\hat{n}\cdot\vec{\sigma}} = \cos\varphi\, I + i \sin\varphi(\hat{n} \cdot \vec{\sigma}).$$

Then, we have $e^{i\varphi_1\hat{n}\cdot\vec{\sigma}} \cdot e^{i\varphi_2\hat{n}\cdot\vec{\sigma}} = e^{i(\varphi_1+\varphi_2)\hat{n}\cdot\vec{\sigma}}$ and $\left(e^{i\phi\vec{n}\cdot\sigma}\right)^m = e^{im\phi\vec{n}\cdot\sigma}$. It should be noted that for every matrix U in $\mathbf{SU}(2)$ there exist an angle φ_U and a unit vector $\hat{n}_U \in \mathbb{R}^3$, such that ([22], page 170)

$$U = e^{i\varphi_U\hat{n}_U\cdot\vec{\sigma}}\,.$$

From the similarity transformations (see identities (3)) it follows that:

$$\begin{aligned} {\sigma_x}^{\alpha} &= H\,{\sigma_z}^{\alpha}\,H, \\ {\sigma_y}^{\alpha} &= {\sigma_z}^{\frac{1}{2}}\,{\sigma_x}^{\alpha}\,{\sigma_z}^{-\frac{1}{2}}, \\ H^{\alpha} &= {\sigma_y}^{\frac{1}{4}}\,{\sigma_z}^{\alpha}\,{\sigma_y}^{-\frac{1}{4}}. \end{aligned}$$

Note that we can also equivalently write ${\sigma_j}^{\alpha} = e^{i\frac{\pi\alpha}{2}}e^{-i\frac{\pi\alpha}{2}\sigma_j}$. So, using our basis (2), it is possible to compute ${\sigma_j}^m$ and H^m for $j \in \{x, y, z\}$ and $m \in \{1, \frac{1}{2}, \frac{1}{4}\}$. These matrices form an interesting family for quantum computation, and are generally used to put a relative phase between $|0\rangle$ and $|1\rangle$. For example, ${\sigma_z}^{\frac{1}{2^n}}$, for integer values of n, are used in Shor's Factorization algorithm [25]. Note that we can also equivalently write ${\sigma_j}^{\alpha} = e^{i\frac{\pi\alpha}{2}}e^{-i\frac{\pi\alpha}{2}\sigma_j}$.

Next, to motivate our proof, we note the connection between real rotations in three dimensions (i.e., elements of $\mathbf{SO}(3)$) and the group we are concerned with, $\mathbf{SU}(2)$. Note that Euler decompositions provide a way to represent a general rotation by an angle 2ϕ about an axis $\hat{n}$, $R_{\hat{n}}(2\phi)$, by a product of rotations about two orthogonal axes. That is,

$$R_{\hat{n}}(2\phi) = R_{\hat{z}}(2\alpha)R_{\hat{y}}(2\beta)R_{\hat{z}}(2\gamma). \quad (4)$$

There is a local isomorphism between $\mathbf{SO}(3)$ and $\mathbf{SU}(2)$. For the same parameters in (4), the following equation is also true:

$$e^{i\phi\hat{n}\cdot\vec{\sigma}} = e^{i\alpha\sigma_z}e^{i\beta\sigma_y}e^{i\gamma\sigma_z}\,. \quad (5)$$

Thus, just as any rotation can be thought of as three rotations about two axes, any element of $\mathbf{SU}(2)$ can be thought of as a product of three matrices, specifically, powers of exponentials of Pauli matrices. In the following section we will show that using the operations in our basis (2), we can approximate any "rotation" about two specific orthogonal axes, and then by Euler decomposition, we will show how all elements of $\mathbf{SU}(2)$ can be approximated.

3. A proof of universality

The proof of universality of our basis will be broken down into two steps. In the first step we show that H and ${\sigma_z}^{\frac{1}{4}}$ form a dense set in $\mathbf{SU}(2)$; i.e. for any element of $\mathbf{SU}(2)$ and desired degree of precision, there exists a finite product of H and ${\sigma_z}^{\frac{1}{4}}$

that approximates it to this desired degree of precision. Next we observe that for universal quantum computation all that is needed is $\Lambda_1(\sigma_x)$ and $\mathbf{SU}(2)$ [4].

For proving density in $\mathbf{SU}(2)$ using our basis, we first show that we can construct elements in our basis which correspond to rotations by angles that are irrational multiples of π in $\mathbf{SO}(3)$ about two orthogonal axes. Once we have these irrational rotations about two orthogonal axes, then the density in $\mathbf{SU}(2)$ follows simply from the local isomorphism between $\mathbf{SU}(2)$ and $\mathbf{SO}(3)$ discussed in the previous section.

The unitary operations $U_1 = {\sigma_z}^{-\frac{1}{4}}\,{\sigma_x}^{\frac{1}{4}}$ and $U_2 = H^{-\frac{1}{2}}\,{\sigma_z}^{-\frac{1}{4}}\,{\sigma_x}^{\frac{1}{4}}\,H^{\frac{1}{2}}$ are exactly computable by our basis. As mentioned in Section 1, there are unit vectors $\hat{n}_1, \hat{n}_2 \in \mathbb{R}^3$ and angles λ_1 and λ_2 such that $U_1 = e^{i\pi\lambda_1\hat{n}_1\cdot\vec{\sigma}}$ and $U_2 = e^{i\pi\lambda_2\hat{n}_2\cdot\vec{\sigma}}$. By calculating the values of $\hat{n}_j$ and λ_j we get $\lambda_1 = \lambda_2 = \lambda$ and

$$\begin{aligned}\cos\lambda\pi = \cos^2\tfrac{\pi}{8} &= \tfrac{1}{2}(1+\tfrac{1}{\sqrt{2}}),\\ \vec{n}_1 &= (\sqrt{2}\cot\tfrac{\pi}{8})\tfrac{\hat{z}-\hat{x}}{\sqrt{2}} + \hat{y},\\ \vec{n}_2 &= (\sqrt{2}\cot\tfrac{\pi}{8})\hat{y} - \tfrac{\hat{z}-\hat{x}}{\sqrt{2}},\end{aligned}$$

where $\hat{n}_j = \vec{n}_j/\|\vec{n}_j\|$ and $\hat{x}, \hat{y}$, and $\hat{z}$ are the unit vectors along the respective axes. One can easily verify that $\vec{n}_1$ and $\vec{n}_2$ are orthogonal (these vectors would need to be normalized when used in exponentiation).

The number $e^{i2\pi\lambda}$ is a root of the irreducible monic polynomial

$$x^4 + x^3 + \frac{1}{4}x^2 + x + 1$$

which is not cyclotomic (since not all coefficients are integers), and thus λ is an irrational number (see Appendix B Theorem B.1). Since λ is irrational, it can be used to approximate any angle φ as $\lambda m \approx \varphi$, for some $m \in \mathbb{N}$. So we have $\left(e^{i\pi\lambda\hat{n}_j\cdot\sigma}\right)^m = e^{im\pi\lambda\hat{n}_j\cdot\sigma} \approx e^{i\pi\varphi\hat{n}_j\cdot\sigma}$.

Fortunately, this is all that is needed. Since, from orthogonality of $\vec{n}_1$ and $\vec{n}_2$, it follows that for any $U \in \mathbf{SU}(2)$ there are angles α, β and γ such that ([22], page 173):

$$U = e^{i\varphi_U\hat{n}_U\cdot\vec{\sigma}} = (e^{i\alpha\hat{n}_1\cdot\vec{\sigma}})(e^{i\beta\hat{n}_2\cdot\vec{\sigma}})(e^{i\gamma\hat{n}_1\cdot\vec{\sigma}})\ . \quad (6)$$

The representation in (6) is clearly analogous to Euler rotations about three orthogonal vectors. Expansion of (6) gives:

$$\cos\phi = \cos\beta\cos(\gamma+\alpha) \quad (7)$$

$$\begin{aligned}\hat{n}\sin\phi = {}& \hat{n}_1\cos\beta\sin(\gamma+\alpha)\\ &+ \hat{n}_2\sin\beta\cos(\gamma-\alpha)\\ &+ \hat{n}_1\times\hat{n}_2\sin\beta\sin(\gamma-\alpha)\end{aligned} \quad (8)$$

For any element of $U \in \mathbf{SU}(2)$ equations (7) and (8) can be inverted to find α, β and γ. For any element of $\mathbf{SU}(2)$ equations (7) and (8) can be inverted to find α, β and γ. Since $\Lambda_1(\sigma_x)$ and $\mathbf{SU}(2)$ form a universal basis for quantum computation [4], it completes the proof of universality of our basis.

There is no guarantee that, in general, it is possible to *efficiently approximate* an arbitrary phase $e^{i\varphi}$ by repeated applications of the available phase $e^{i\pi\lambda}$. But using an argument similar to the one presented in [1], we can show that for the given λ (as defined in (3)), for any given $\varepsilon > 0$, with only poly$(\frac{1}{\varepsilon})$ iterations of $e^{i\pi\lambda}$ we can get $e^{i\varphi}$ within ε. However, since our basis is already proven to be universal, one can make use of an even better result. As it is shown by Kitaev [16] and Solovay and Yao [26], every universal quantum basis $\mathcal{B}$ is efficient, in the sense that any unitary operation in U(2^m), for constant m, can be approximated within ε by a circuit of size poly-log$(\frac{1}{\varepsilon})$ over the basis $\mathcal{B}$.

4. A fault-tolerant realization of ${\sigma_z}^{\frac{1}{4}}$

We provide a simple scheme for the fault-tolerant realization of the ${\sigma_z}^{\frac{1}{4}}$ gate. The method describes a general procedure that works for any quantum code for which the elements of the normalizer group can be implemented fault-tolerantly and involves the creation of special eigenstates of unitary transformations.

To perform ${\sigma_z}^{\frac{1}{4}}$ fault-tolerantly we use the following state:

$$|\varphi_0\rangle \equiv {\sigma_z}^{\frac{1}{4}}H|0\rangle = \frac{|0\rangle + e^{i\frac{\pi}{4}}|1\rangle}{\sqrt{2}}\ , \quad (9)$$

(for which we later present the preparation process). To apply ${\sigma_z}^{\frac{1}{4}}$ to a general single qubit state $|\psi\rangle$ using this special state $|\varphi_0\rangle$, first apply $\Lambda_1(\sigma_x)$ from $|\psi\rangle$ to $|\varphi_0\rangle$. See Figure 1. Then measure the second qubit ($|\varphi_0\rangle$) in the computation basis. If the result is $|1\rangle$,

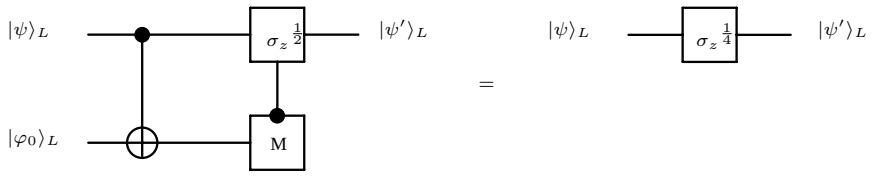

Figure 1. Implementing $\sigma_z{}^{\frac{1}{4}}$ fault-tolerantly.

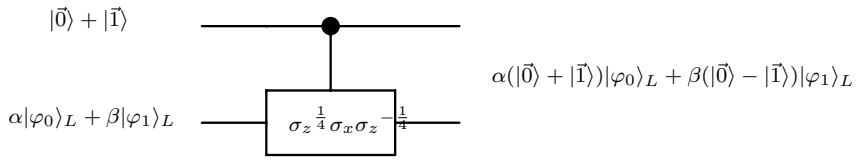

Figure 2. Creation of the $|\varphi_0\rangle$ eigenstate.

apply $\sigma_z{}^{\frac{1}{2}}$ to the first qubit ($|\psi\rangle$). This leads to the desired operation, as demonstrated in the following:

$$\begin{aligned} |\psi\rangle \otimes |\varphi_0\rangle \quad &= \quad (\alpha|0\rangle + \beta|1\rangle) \otimes \tfrac{|0\rangle + e^{i\frac{\pi}{4}}|1\rangle}{\sqrt{2}} \\ &\xrightarrow{\Lambda_1(\sigma_x)} \quad (\alpha|0\rangle + e^{i\frac{\pi}{4}}\beta|1\rangle) \otimes \tfrac{|0\rangle}{\sqrt{2}} \\ &\quad +(\alpha|0\rangle + e^{-i\frac{\pi}{4}}\beta|1\rangle) \otimes e^{i\frac{\pi}{4}}\tfrac{|1\rangle}{\sqrt{2}} \\ &= \quad \sigma_z{}^{\frac{1}{4}}|\psi\rangle \otimes \tfrac{|0\rangle}{\sqrt{2}} + \sigma_z{}^{-\frac{1}{4}}|\psi\rangle \otimes e^{i\frac{\pi}{4}}\tfrac{|1\rangle}{\sqrt{2}}. \end{aligned}$$

Clearly, the above analysis shows that all that is necessary to perform $\sigma_z{}^{\frac{1}{4}}$ fault tolerantly is the state $|\varphi_0\rangle$ and the ability to do $\Lambda_1(\sigma_x)$ and $\sigma_z{}^{\frac{1}{2}}$ fault-tolerantly. For CSS codes, $\Lambda_1(\sigma_x)$, H and $\sigma_z{}^{\frac{1}{2}}$ can be done fault-tolerantly [24, 13]. We next show how to generate the state $|\varphi_0\rangle$ fault-tolerantly.

Fault tolerant creation of certain particular encoded eigenstates has been discussed[24, 18]. We present it in a more general way: suppose that the fault-tolerant operation U_η operates as follows:

$$U_\eta|\eta_i\rangle = (-1)^i|\eta_i\rangle \tag{10}$$

on the states $|\eta_i\rangle$. Thus, U_η has the states $|\eta_i\rangle$ as eigenvectors with ± 1 as the eigenvalues. Suppose we have access to a vector $|\psi\rangle$ such that:

$$|\psi\rangle = \alpha|\eta_0\rangle + \beta|\eta_1\rangle. \tag{11}$$

We show that using only bitwise operations, measurements, and this $|\psi\rangle$, the eigenvectors $|\eta_i\rangle$ can be obtained. Now, to get the eigenvector of U_η we make use of a $|\mathsf{cat}\rangle$ state:

$$|\mathsf{cat}\rangle = \tfrac{1}{\sqrt{2}}(|00...0\rangle + |11...1\rangle) = \tfrac{1}{\sqrt{2}}(|\vec{0}\rangle + |\vec{1}\rangle). \tag{12}$$

See Figure 2. Applying $\Lambda_1(U_\eta)$ bitwise, on $|\mathsf{cat}\rangle \otimes |\psi\rangle$ we obtain:

$$|\mathsf{cat}\rangle \otimes |\psi\rangle \xrightarrow{\Lambda_1(U_\eta)} \alpha(\tfrac{|\vec{0}\rangle+|\vec{1}\rangle}{\sqrt{2}})|\eta_0\rangle + \beta(\tfrac{|\vec{0}\rangle-|\vec{1}\rangle}{\sqrt{2}})|\eta_1\rangle. \tag{13}$$

A fault-tolerant measurement can be made to distinguish $\frac{|\vec{0}\rangle+|\vec{1}\rangle}{\sqrt{2}}$ from $\frac{|\vec{0}\rangle-|\vec{1}\rangle}{\sqrt{2}}$ [24]. This measurement can be repeated to verify that you have it correct.

The fault-tolerant version of $\sigma_z{}^{\frac{1}{4}}$ needs the state $|\varphi_0\rangle$, which can be generated using this formalism. In fact, $|\varphi_0\rangle$ is an eigenstate of $U_\varphi = \sigma_z{}^{\frac{1}{4}}\sigma_x\sigma_z{}^{-\frac{1}{4}}$. By commutation properties of the $\sigma_z{}^{-\frac{1}{4}}$ operator, it is shown that U_φ can be realized with elements only from the normalizer group:

$$U_\varphi = \sigma_z{}^{\frac{1}{4}}\sigma_x\sigma_z{}^{-\frac{1}{4}} = e^{i\frac{\pi}{4}}\sigma_z{}^{\frac{1}{2}}\sigma_x. \tag{14}$$

Since $\sigma_z{}^{\frac{1}{2}}$ and σ_x can be done fault-tolerantly, so can U_φ. We have claimed that $|\varphi_0\rangle$ (9) is an eigenvector, and now we state the other eigenvector; i.e.,

$$|\varphi_1\rangle \equiv \sigma_z{}^{\frac{1}{4}}H|1\rangle = \frac{|0\rangle - e^{i\frac{\pi}{4}}|1\rangle}{\sqrt{2}} \tag{15}$$

One can verify now that these $|\varphi_i\rangle$ are eigenvectors:

$$\begin{aligned} U_\varphi|\varphi_i\rangle &= \sigma_z{}^{\frac{1}{4}}\sigma_x\sigma_z{}^{-\frac{1}{4}}|\varphi_i\rangle \\ &= \sigma_z{}^{\frac{1}{4}}\sigma_x\sigma_z{}^{-\frac{1}{4}}(\sigma_z{}^{\frac{1}{4}}H|i\rangle) = \sigma_z{}^{\frac{1}{4}}\sigma_x H|i\rangle \\ &= \sigma_z{}^{\frac{1}{4}}H\sigma_z|i\rangle = \sigma_z{}^{\frac{1}{4}}H(-1)^i|i\rangle = (-1)^i|\varphi_i\rangle \end{aligned} \tag{16}$$

Since the $|\varphi_i\rangle$ vectors are orthogonal, any single qubit state $|\psi\rangle$ can be represented as a sum of the $|\varphi_i\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha'|\varphi_0\rangle + \beta'|\varphi_1\rangle. \quad (17)$$

So, all the necessary ingredients are here: $|\psi\rangle$, and an appropriate fault-tolerant operation, U_φ. If the outcome gives $|\varphi_1\rangle$ rather than $|\varphi_0\rangle$ we can flip the state:

$$|\varphi_0\rangle = \sigma_z|\varphi_1\rangle = \sigma_z\frac{|0\rangle - e^{i\frac{\pi}{4}}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i\frac{\pi}{4}}|1\rangle}{\sqrt{2}}. \quad (18)$$

Shor's implementation of Toffoli [24] also uses a special case of this general procedure. For performing Toffoli one uses $U = \Lambda_1(\sigma_z) \otimes \sigma_z$ to get the eigenstates:

$$\begin{aligned} |\mathsf{AND}\rangle &= \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle) \\ |\mathsf{NAND}\rangle &= \frac{1}{2}(|001\rangle + |011\rangle + |101\rangle + |110\rangle) \end{aligned}$$

Shor uses the $|\psi\rangle$ state of:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|\mathsf{AND}\rangle + |\mathsf{NAND}\rangle) \\ &= (H|0\rangle) \otimes (H|0\rangle) \otimes (H|0\rangle). \end{aligned}$$

Thus the special state in [24] can be obtained by the same general procedure.

5. Universality of Shor's basis

5.1. Equivalence between $\{\Lambda_1({\sigma_z}^{\frac{1}{2}}), H\}$ and Shor's basis'

Kitaev ([16], Lemma 4.6) has provided a proof for the universality of the basis $Q_1 := \{\Lambda_1({\sigma_z}^{\frac{1}{2}}), H\}$. This basis is equivalent to Shor's fault-tolerant basis $\{\Lambda_2(\sigma_x), {\sigma_z}^{\frac{1}{2}}, H\}$, as observed in [16]. We give one demonstration of this equivalence here for completeness. This equivalence was also showed independently by Aharonov and Ben-Or (in journal version of [2]).

To construct Q_1 from Shor's basis, it suffices to construct $\Lambda_1({\sigma_z}^{\frac{1}{2}})$. First we show that the operations $\Lambda_2(\sigma_z)$ and $\Lambda_2(\sigma_y)$ can be implemented exactly using gates from Shor's basis (I_{2^n} is the identity operation on n qubits.):

$$\begin{aligned} H_z &\equiv H{\sigma_z}^{-\frac{1}{2}}H{\sigma_z}^{\frac{1}{2}}H \\ \Lambda_2(\sigma_z) &= (I_4 \otimes H)\Lambda_2(\sigma_x)(I_4 \otimes H) \\ \Lambda_2(\sigma_y) &= (I_4 \otimes H_z)\Lambda_2(\sigma_x)(I_4 \otimes H_z), \end{aligned}$$

Next, as shown in Figure 3, $\Lambda_1({\sigma_z}^{\frac{1}{2}})$ can be implemented using the identity: $\sigma_x\sigma_y\sigma_z = iI_2$. This reduction also shows that the universality of Q_1 implies the universality of Shor's basis.

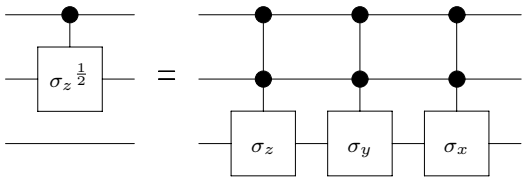

Figure 3. Constructing Q_1 from Shor's basis.

Conversely, to construct Shor's basis from Q_1, it suffices to construct the Toffoli gate $\Lambda_2(\sigma_x)$. Note that $\Lambda_1({\sigma_x}^{\pm\frac{1}{2}}) = (I_2 \otimes H)\Lambda_1({\sigma_z}^{\pm\frac{1}{2}})(I_2 \otimes H)$. Figure 4 gives the circuit construction of Toffoli (see Lemma 6.1 of [4] for a systematic construction of this circuit).

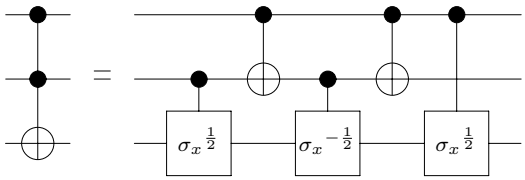

Figure 4. Constructing $\Lambda_2(\sigma_x)$ from Q_1.

5.2. An alternate proof

An alternative proof, which makes use of irrational "rotations" about orthogonal axes, is presented in this section for the universality of each of the above two basis'. From either one of these sets, the following triplet of double-qubit gates is constructible:

$$G \equiv \{\Lambda_1({\sigma_x}^{\frac{1}{2}}), \Lambda_1({\sigma_z}^{\frac{1}{2}}), S\}$$

where S is the swap gate: $S|ab\rangle = |ba\rangle$ for any single-qubit states $|a\rangle, |b\rangle$, which can be constructed as

$$S = \Lambda_1(\sigma_x)(H \otimes H)\Lambda_1(\sigma_x)(H \otimes H)\Lambda_1(\sigma_x).$$

For future reference, note that each of the matrices in G are symmetric. Hence for any matrix M that is constructible from this set, so is its transpose M^T.

It will be shown that any gate in the set

$$\Sigma := \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & & & \\ 0 & & \mathbf{SU}(3) & \\ 0 & & & \end{array}\right)$$

can be approximated to arbitrary precision by a two-qubit circuit consisting only of gates from the set G. I.e. the set G under regular matrix multiplication generates a set dense in Σ. From this set all single-qubit unitary operations **SU**(2) can be approximated, which along with $\Lambda_1(\sigma_x)$, has been shown [4] to be a universal set of gates.

Though the correspondence is not a strict mathematical correspondence, it will be useful to make an analogy between real rotations in 3-dimensional space, and gates constructible from G. Define the following 6 elements of $\langle G\rangle$:

$$\begin{aligned} \rho_x &:= \Lambda_1({\sigma_x}^{\frac{1}{2}})\Lambda_1({\sigma_z}^{\frac{1}{2}})^{-1}, \\ \rho_y &:= S\rho_x^{-1}S, \\ \rho_z &:= \Lambda_1(\sigma_x)\rho_y^{-1}\Lambda_1(\sigma_x), \\ \rho_1 &:= \rho_z^{-1}\Lambda_1(\sigma_x)\Lambda_1({\sigma_z}^{\frac{1}{2}})\rho_z, \\ \rho_2 &:= \rho_x\rho_y, \\ \rho_3 &:= \rho_1\rho_2\rho_1^{-1}. \end{aligned}$$

(Each inverse in the above definitions are obtainable from G, since each element of G is of finite group order.) Since ρ_2 and ρ_3 are unitary, they can be unitarily diagonalized:

$$\begin{aligned} \rho_2 &= g_2 D(1, 1, e^{-i2\pi c}, e^{i2\pi c})g_2^{-1}, \\ \rho_3 &= g_3 D(1, 1, e^{-i2\pi c}, e^{i2\pi c})g_3^{-1}, \end{aligned}$$

where g_2, g_3 are some unitary matrices (not necessarily in $\langle G\rangle$), D is a diagonal matrix with the given ordered quadruplet as the entries along the diagonal, and $e^{i2\pi c} = \frac{1+i\sqrt{15}}{4}$ for some $c \in \mathbb{R}$. The minimum monic polynomial for $e^{i2\pi c}$ over the set of rational numbers is

$$m_{e^{i2\pi c}}(x) = x^2 - \frac{1}{2}x + 1 \notin \mathbb{Z}[x]$$

and thus $c \notin \mathbb{Q}$ (see Appendix B, Theorem B.1). It follows that successive powers of ρ_2 and ρ_3 can approximate matrices of the forms

$$\rho_2^{n_2} \approx g_2 D(1, 1, e^{-i\theta_2}, e^{i\theta_2})g_2^{-1} \quad (19)$$

$$\rho_3^{n_3} \approx g_3 D(1, 1, e^{-i\theta_3}, e^{i\theta_3})g_3^{-1} \quad (20)$$

for any $\theta_2, \theta_3 \in \mathbb{R}$. The powers n_2 and n_3 are functions of θ_2 and θ_3, as well as the desired degree of accuracy.

The operators ρ_1, ρ_2, and ρ_3 fix the (unnormalized) states $|01\rangle - |10\rangle$, $|01\rangle + |10\rangle + |11\rangle$, and $-|01\rangle - |10\rangle + 2|11\rangle$, resp. which form an orthogonal set of states. Motivated by considering these 3 operations to be rotations about 3 orthogonal vectors, a change of basis is performed into this basis (while mapping the state $|00\rangle$ to itself). Under this change of basis, equations (19) and (20) are expressed as:

$$\hat{\rho}_2^{n_2} \approx \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\theta_2) & 0 & \alpha\sin(\theta_2) \\ 0 & 0 & 1 & 0 \\ 0 & -\alpha^*\sin(\theta_2) & 0 & \cos(\theta_2) \end{pmatrix}$$

$$\hat{\rho}_3^{n_3} \approx \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\theta_3) & -\beta^*\sin(\theta_3) & 0 \\ 0 & \beta\sin(\theta_3) & \cos(\theta_3) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where $\alpha \equiv \frac{1+2i}{\sqrt{5}}$ and $\beta \equiv \frac{1+3i}{\sqrt{10}}$, which like $e^{i2\pi c} = \frac{1+i\sqrt{15}}{4}$ above, are also seen to not be roots of unity.

Given any $\gamma \in \mathbb{C}$, $|\gamma| = 1$, define the following single-parameter group of matrices:

$$M_\gamma(\theta) \equiv \begin{pmatrix} \cos(\theta) & -\gamma^*\sin(\theta) \\ \gamma\sin(\theta) & \cos(\theta) \end{pmatrix}.$$

If γ is not a root of unity, then it is straightforward to show that the set of matrices $\left\{ M_\gamma(\theta)^T, M_\gamma(\theta) \middle| \theta \in \mathbb{R} \right\}$ generates a dense subset of $\mathbf{SU}(2)$. Given this, and the fact that any element of $\mathbf{SU}(3)$ can be decomposed into a product of $\mathbf{SU}(2)$ operations acting on orthogonal subspaces[20], it follows that the set

$$\left\{ \hat{\rho}_2^T, \hat{\rho}_2, \hat{\rho}_3^T, \hat{\rho}_3 \right\}$$

generates a dense subset of Σ. Since the previous change of basis bijectively and continuously maps Σ onto itself, the operators G in the original basis generates a dense subset of Σ. $\square$

Acknowledgments

We thank Alexi Kitaev and Peter Shor for helpful discussions on the subject of this paper. We are grateful to Dorit Aharonov for her comments on an earlier version of this work. We are grateful to Brian Albright for discussions leading to our construction of rotations by angles corresponding to irrational multiples of π, and to Terence Tao for a suggestion that led to the development of the cyclotomic/irrational number theorem.

References

[1] L. M. Adleman, J. Demarrais, and M. D. A. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, October 1997.

[2] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing, STOC'97*, pages 46–55. ACM Press, New York, NY, USA, 1997.

[3] A. Barenco. A universal two-bit gate for quantum computation. *Proceedings of the Royal Society of London, Series A*, 449(1937):679–683, June 1995.

[4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, November 1995.

[5] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, October 1997.

[6] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, August 1996.

[7] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Physical Review Letters*, 74(20):4091–4094, 15 May 1995.

[8] D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London Ser. A*, 425(1868):73–90, 1989.

[9] P. Domokos, J. M. Raimond, M. Brune, and S. Haroche. Simple cavity-QED two-bit universal quantum logic gate: The principle and expected performances. *Physical Review A*, 52(5):3554–3559, November 1995.

[10] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Prentice-Hall, Inc., Upper Saddle River, N.J., 1999. Second Edition.

[11] N. Gershenfeld and I. L. Chuang. Bulk spin-resonance quantum computation. *Science*, 275(5298):350–356, 17 January 1997.

[12] D. G. Gory, A. F. Fahmy, and T. F. Havel. Ensemble quantum computing by nuclear magnetic resonance spectroscopy. *Proc. Natl. Acad. Sci.*, 94:1634–1639, 1997.

[13] D. Gottesman. Theory of fault-tolerant quantum computation. *Physical Review A*, 57(1):127–137, January 1998.

[14] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, 14 July 1997.

[15] B. E. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393(6681):133–137, 14 May 1998.

[16] A. Y. Kitaev. Quantum computation: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[17] E. Knill, R. Laflamme, and W. H. Zurek. Accuracy threshold for quantum computation. LANL eprint quant-ph/9611025, 1996.

[18] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279(5349):342–3245, 16 January 1998.

[19] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Demonstration of a fundamental quantum logic gate. *Physical Review Letters*, 75(25):4714–4717, 18 December 1995.

[20] F. D. Murnaghan. *The Unitary and Rotation Groups*. Spartan Books, Washington, D.C., 1962.

[21] J. Preskill. Reliable quantum computers. *Proceedings of the Royal Society of London, Series A*, 454(1969):385–410, 8 January 1998.

[22] J. J. Sakurai. *Modern Quantum Mechanics*. Addison Wesley, Reading, Mass., 1994.

[23] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493–2496, October 1995.

[24] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Annual Symposium on Foundations of Computer Science, FOCS'96*, pages 56–65. IEEE Computer Society Press, Los Alamitos, CA, USA, 1996.

[25] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[26] R. Solovay and A. Yao. Preprint, 1996.

[27] A. M. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793–797, 29 July 1996.

[28] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.*, 75(25):4710–4713, 18 December 1995.

[29] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo. Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures. LANL eprint quant-physics/9905096, 1999.

A. Shor's basis and $\{ H, \sigma_z{}^{\frac{1}{4}}, \Lambda_1(\sigma_x) \}$ are not equivalent

In this appendix we show that Shor's basis and our basis $\{ H, \sigma_z{}^{\frac{1}{4}}, \Lambda_1(\sigma_x) \}$ are not equivalent. In fact, every gate in Shor's basis can be exactly represented by a circuit over our basis. First, the following identity shows that our basis can exactly implement any gate from the Q_1 basis introduced in Section 5.1:

$$\begin{aligned}\Lambda_1(\sigma_z{}^{\frac{1}{2}}) &= \left(I \otimes \sigma_z{}^{-\frac{1}{4}}\right) \Lambda_1(\sigma_x) \\ &\quad \left(I \otimes \sigma_z{}^{-\frac{1}{4}}\right) \Lambda_1(\sigma_x) \\ &\quad \left(\sigma_z{}^{\frac{1}{4}} \otimes \sigma_z{}^{\frac{1}{2}}\right).\end{aligned}$$

Hence, as proved in the same section, it can exactly implement any gate from Shor's basis. We prove that the converse is not true. Toward this end, we show that the unitary operation $\sigma_z{}^{\frac{1}{4}}$, can be computed exactly by our basis but not by Shor's basis. First we prove a useful Lemma about unitary operations computable exactly by Shor's basis. Note that the set of integer complex numbers is the set $\mathbb{Z} + i\mathbb{Z}$ of the complex numbers with integer real and imaginary parts.

Lemma A.1 *Suppose that the unitary operation $U \in \mathbf{U}(2^m)$ is the transformation performed by a circuit $\mathcal{C}$ defined over Shor's basis with m inputs. Then U is of the form $\frac{1}{\sqrt{2}^\ell} M$, where M is a $2^m \times 2^m$ matrix with only complex integer entries.*

Proof. Suppose that $g_1, \ldots, g_t$ are the gates of $\mathcal{C}$. Each gate g_j can be considered as a unitary operation in $\mathbf{U}(2^m)$ by acting as an identity operator on the qubits that are not inputs of g_j. Let the matrix $M_j \in \mathbf{U}(2^m)$ represent g_j. Then $U = M_t \cdots M_1$. If g_j is a $\sigma_z{}^{\frac{1}{2}}$ gate then M_j is a diagonal matrix with 1 or i on its diagonal. If g_j is a Toffoli gate then M_j is a permutation matrix (which is a 0–1 matrix). Finally, if g_j is a Hadamard gate, then $M_j = \frac{1}{\sqrt{2}} M_j{}'$, where the entries of $M_j{}'$ are integers. This completes the proof. □

Now since $\sigma_z{}^{\frac{1}{4}} = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1+i \end{pmatrix}$, by Lemma A.1 it cannot be realized exactly by gates from Shor's basis.

B. The Cyclotomic/Rational Number Theorem

Theorem B.1 *For any $c \in \mathbb{R}$, the following two statements are logically equivalent:*

(a) The minimum monic polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ for $\alpha \equiv e^{i2\pi c}$ exists and is cyclotomic.

(b) $c \in \mathbb{Q}$.

Proof:

A number of algebraic theorems will be taken for granted in this proof, in particular, properties of cyclotomic polynomials $\Phi_n(x)$. See, for instance, Dummit and Foote [10] for a more thorough discussion of these polynomials, as well as general properties of polynomial rings.

Assume $m_\alpha(x)$ exists and $m_\alpha(x) = \Phi_n(x)$ for some $n \in \mathbb{Z}^+$.

$$\begin{aligned}0 &=^{1} m_\alpha(\alpha) \\ &=^{2} \Phi_n(\alpha) \\ &=^{3} \prod_{d|n} \Phi_d(\alpha) \\ &=^{4} \alpha^n - 1 \\ &=^{5} e^{i2\pi cn} - 1.\end{aligned}$$

$nc \in \mathbb{Z}$. Thus $c \in \mathbb{Q}$.

Conversely, assume $c \in \mathbb{Q}$. $c = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$. $m_\alpha(x)$ exists, since $\alpha^q - 1 = e^{i2\pi cq} - 1 = e^{i2\pi p} - 1 = 0$. Moreover, $m_\alpha(x)$ divides $x^q - 1 = \prod_{d|q} \Phi_d(x)$ in $\mathbb{Q}[x]$. $m_\alpha(x) \propto \Phi_n(x)$ for some $n|q$. Since both are monic, $m_\alpha(x) = \Phi_n(x)$. □

[1] Definition of $m_\alpha(x)$

[2] By assumption.

[3] 0 times anything is 0.

[4] Property of cyclotomic polynomials.

[5] Definition of α.